PCT/IB 0 4 / 0 2 0 1 1
(1 0. 06. 04)

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 18 March 2004

tents Form 1/77

Patents Act 1977
Rule 16)

THE PATENT OFFICE
D
21 JUN 2003
NEWPORT

The Patent Office

1/77

Request for grant of a patent
(See notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

Your reference PHGB030098GBP

21 JUN 2003

Patent application number
(The Patent Office will fill in this pa 0314557.0

23JUN03 E816989-1 D03008
P01/7700 0.00-0314557.0

Full name, address and postcode of the or of each applicant (*underline all surnames*)

KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN
THE NETHERLANDS

Patents ADP Number (*if you know it*) 07419294001

If the applicant is a corporate body, give the country/state of its incorporation THE NETHERLANDS

Title of the invention IMPROVED REDUCTION CALCULATIONS

Name of your agent (*if you have one*)
"Address for service" in the United Kingdom to which all correspondence should be sent (*including the postcode*)

Philips Intellectual Property and Standards
Cross Oak Lane
Redhill
Surrey RH1 5HA

Patents ADP number (*if you know it*) 08359655001

If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (*if you know it*) the or each application number

Country	Priority Application number (*if you know it*)	Date of filing (*day/month/year*)

If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing (*day/month/year*)

Is a statement of inventorship and of right to grant of a patent required in support of this request? (*Answer "Yes" if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.

See note (d))

YES

Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document.

Continuation sheets of this form	
Description	9
Claims(s)	5
Abstract	1
Drawings	5

only

If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

Request for substantive examination (*Patents Form 10/77*)

Any other documents (*Please specify*)

I/We request the grant of a patent on the basis of this application.

Signature Richard Turner Date 20.6.3

Name and daytime telephone number of person to contact in the United Kingdom 01293 815492 (R. Turner)

rning

r an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or munication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be med if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, ion 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the nt Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same ntion and either no direction prohibiting publication or communication has been given, or any such direction has been ked.

s

If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

Write your answers in capital letters using black ink or you may type them.

If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

If you have answered "Yes" Patents Form 7/77 will need to be filed.

Once you have filled in the form you must remember to sign and date it.

For details of the fee and ways to pay please contact the Patent Office.

DESCRIPTION

IMPROVED REDUCTION CALCULATIONS

The present invention relates to a method of performing a reduction operation and to apparatus for performing a reduction operation.

Elliptic Curve Cryptography (ECC) involves the use of calculations on an elliptic curve relationship over GF(p) and requires the multiplication of long integers which are carried out repeatedly during the implementation of, for example, public key algorithms in cryptographic processors.

Typically, the multiplication operations must be carried out many hundreds of times to complete an encryption or decryption operation, and so it is important that the cryptographic devices that perform these operations execute the long multiplications quickly using a high speed multiplier.

Increasingly, such cryptographic algorithms are used in electronic devices for example smart cards, and in these applications processing capability and power consumption is severely limited.

One conventional calculation method is the Quisquater system which operates on the Most Significant Word using the operation

$R'=R+(-N'*MSW)$,

where N' is a special multiple of N. In fact, -N' is used in its 2's complement notation.

The reduction operation is inefficient, and the result may be too large, necessitating the addition of (-N') to R'.

Another conventional calculation method is the Mongomery system which operates on the Least Significant Word using the operation

$R'=R+N*Q$

where $Q = LSW*M \bmod 2n$.

Again the reduction operation is inefficient and might be one bit too large requiring restoration by subtraction of N.

It is therefore an object of the present invention to provide a more efficient reduction operation.

It is also an object of the present invention to provide a reduction operation with a lower number of multiplication operations.

It is also an object of the present invention to provide a reduction operation which provides fewer overflows in the calculation operations.

It is also an object of the present invention to provide a reduction operation in which the reduction operation is completed faster.

According to one aspect, the present invention provides a method of performing a reduction operation in a cryptographic calculation, the method comprising selecting a modulus having a first section with a plurality of "1" Most Significant Word states and a second section which comprises a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and operating a reduction operation on the modulus/multiple.

By this selection of a particular form of a modulus/multiple for use in the calculation, the reduction operation involves fewer multiplication operations.

Thus a significant benefit provided by the present invention is that the time taken to complete the entire calculating operation is reduced.

Moreover, the degree of security afforded by the method of the present invention is maintained as compared to conventional cryptographic methods.

Preferably the method comprises monitoring the number of leading "1"s to determine if the number is less than (k-2). Advantageously, when the number of leading "1"s is less than (k-2), the next calculation is initiated.

Thus a further advantage of the present invention is that a number of multiplication operations can be processed simultaneously, thereby reducing the time taken to complete calculating operations.

In one embodiment of the present invention for 192-bit ECC and a word size for 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.

In another embodiment of the present invention for 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

In another embodiment of the present invention for 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and second section of 54 bits.

The invention can also work with a number of moduli, which have less significant bits than a multiple of the word size. In that case, the system works with a multiple of the modulus, which has the required number of leading 1's. Only at the very last end, the result has to be reduced to the original (smaller) modulus.

In one preferred arrangement, the method of the present invention utilises modulus, consisting of m words with all the words except the Least Significant Word (LSW) consisting of "1"s and the LSW has, for example, ten leading "1"s can be any number but bearing in mind the larger it is, then the less often an additional reduction is required.

According to another aspect, the present invention provides a computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of the present invention when said product is run on a computer.

According to another aspect, the present invention provides a computer program directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of the present invention when said program is run on a computer.

According to another aspect, the present invention provides a carrier, which may comprise electronic signals, for a computer program embodying the present invention.

According to another aspect, the present invention provides electronic distribution of a computer program product, or a computer program, or a carrier of the present invention.

According to another aspect, the present invention provides apparatus for performing a reduction operation in a cryptographic calculation, the apparatus comprising means to select a modulus or a multiple of a modulus having a first section with a plurality of "1" states and a second section having

a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus.

In order that the present invention may more readily be understood, a description is now given, by way of example only, reference being made to the accompanying drawings, in which:-

Figure 1 is an application of the present invention in a smart card;

Figure 2 is a schematic drawing of a reduction operation embodying the present invention for 192-bit ECC and 64-bit words;

Figure 3 is a schematic drawing of another reduction operation of the present invention for 128-bit ECC and 64-bit words;

Figure 4 is a schematic drawing of another reduction operation of the present invention for 256-bit ECC and 64-bit words;

Figure 5 is a hardware implementation of the present invention.

Figure 1 shows a block diagram of a hardware implementation of the present invention incorporating a smart card 50 with the following components:

- Microcontroller 51 for general control to communicate with the outside world via the interface. It sets pointers for data in RAM/ROM and starts the coprocessor.
- Interface to the outside world, for contact with smart cards e.g. according to ISO-7816-3.
- A Read Only Memory (ROM) 52 for the program of the microcontroller.
- A Programmable Read Only Memory (Flash or EEPROM) 53 for the non-volatile storage of data or programs.
- RAM 54 for storage of volatile data, e.g for storage of intermediate results during calculations.
- Coprocessor 55 dedicated to perform special high-speed tasks for ECC or RSA calculations. When a task is ready, control is returned to the microcontroller.

In a variant, the present invention is implemented in software with a microprocessor, ALU to provide add, subtract, shift operations with programming of the controller to provide control logic, and degree detection by shift registers.

There is shown in Figure 2 a reduction operation of the present invention which is performed with a modulus comprising in total 192 bit words and having a first section which has all "1" states being two 64-bit words and 10 bits. The second section of the modulus is 54 bits and can be any number provided that the total number is a prime. The bigger the number, the less often that an additional reduction is required.

In general, N can be written as:

$$N = n_{m-1}B^{m-1}+\ldots n_1B+n_0 \quad (B=2^{64})$$

The special requirements for the selection of N are:

- $n1\ldots n_{m-1}$ are fixed and contain only 1's ($n_1=\ldots n_{m-1}=B-1$).
- n_0 is general except for k MSBs which are also 1, leaving 64-k bits free to choose.

Then N is written as

$N=B^m-B+n_0=B^m-n_0'$ with $n_0'= B-n_0$

Let R be the result, which has to be reduced by 1 word.

$R=r_mB^m+r_{m-1}B^{n-1}+\ldots r_1B+r_0$

Reduce the result by subtraction of the product r_mN from R as follows:

$R'= R - r_m.N$

$=r_mB^m+r_{m-1}B^{m-1}+\ldots r_1B+r_0-r_m(B^m-B+n_0)$

$=r_{m-1}B^{m-1}+\ldots+r_2B^2+r_1B+r_0+r_m.(B-n_0)=(R-r_mB^m)+r_m.n_0'$

This means that, for the reduction, omit the word r_m and add to the Least Significant Word r_0 the product $r_m.n_0'$. The reduction implies only one multiplication instead of the normal m multiplications.

n_0' is always positive, since $n_0<B$. The result is also always positive.

Instead of n_0, store and use n_0'.

In some cases, the result is 1 bit too large. Then it is necessary to subtract N again.

$R'=(B^m+r_{m-1}B^{m-1}+\ldots+r_1B+r_0)-(B^m- n_0')=r_{m-1}B^{m-1}+\ldots+r_1B + (r_0+ n_0') = (R-B^m)+ n_0'$.

So, we have only to add n_0' and discard the overflow bit B^m.

For every multiplication by one word, do such a reduction. Alternatively, do first all multiplications and then the reductions. The last method is

described here. The description below is for 192-bit ECC and a 64-bit word size (m=3).

$N = B^3 - B + n_0 = B^3 - n_0'$; $2^9 \leq n_0 < B$ ($B=2^{64}$).

R is the result of the multiplication of three 64-bit words by also three 64-bit words, which results in 6 words ($r_0 \ldots r_5$).

Then the reduction is done as follows:

- Multiplication of n_0' by r_4 and adding r_1 (being step S1);
- Multiplication of n_0' by r_5 and adding r_2, and the carry c of the previous multiplication. Moreover r_3 is added to the upper part of the multiplication. The result consists of the lower half again called r_2 and the upper half q (step S2) ;
- Multiplication of q by n_0' and adding r_0 and adding the new r_1 to the upper part (step S3);
- When the last multiplication gives an overflow, the overflow is added to r_2 e.g by the multiplication of n_0' by 0 (to give 0), the addition of r_1 (gives r_1 as lower half) and the addition of r_2 to the upper part, i.e. the overflow bit) (step S4);
- When this gives again an overflow (i.e. only when r_2 consists of all-ones (chance 2^{-64})), n_0' is added (step S5).
- This can be done by the multiplication of n_0' by 1, and adding r_0 to the lower half of r_1 to the upper half.

The carry of the second multiplication (q) is used as multiplicand in the next multiplication, and can be enlarged by 1 bit.

When the input r_1 to the multiplication of $n_0'q$ does not have 8 leading ones (the probability being less than 1/256), there will be no overflow, since $n_0'q$ has at least 8 leading zeros because of n_0'. In that case, the program does not wait for the overflow to proceed.

Handling of overflows involves time, which has to be minimised wherever possible. Accordingly, n_0 has a number of leading ones (k), so n_0' has at least k-1 leading zeros.

Thus, the product $n_0'c_2$ has at least k-2 leading zeros, since q might be enlarged by 1 bit.

In order to produce an overflow, the addition of $B.c_0+r_0$ has to have at least k-2 leading ones and a carry c from the lower bits.

The probability that this will happen is less than $2^{-(k-2)}$. Therefore by making k high, the likelihood of an overflow is very small.

The probability of the second overflow is extremely small (2^{-64}), since r_2 has to consist completely of ones.

In practice, a pipelined multiplier is used to provide efficient calculation operations, so a number of multiplications are being processed at the same time. It takes a few clock cycles to get the result from the multiplier. When it is necessary to wait to determine whether an overflow occurs, the next multiplications cannot begin until the overflow has been calculated. Thus r_1 is monitored and if it does not have k-2 leading "1"s there will be no overflow a few cycles later so the next multiplication can be started.

There is shown in Figure 3 a different embodiment for 128-bit ECC and a word size of 64-bit incorporating a modulus N having 128 bits.

In this embodiment,

$N=B^2-B+n_0=B^2-n_0'$; $2^9 \leq n_0 < B$.

The operands have to be in normal space.

Then the reduction is done as follows:

- Multiplication of n_0' by r_3 and adding r_1. Also r_2 is added to the upper part of the multiplication (step S10); The result consists of the lower half again called r_1 and the upper half called q.
- Multiplication of q by n_0' and adding r_0 and adding the new r_1 to the upper part (step S11);
- When the last multiplication gives an overflow then we add n_0' (step S12), e.g. by the multiplication/addition $n_0'.1+B.r_1+r_0$.

There is shown in Figure 4 a different embodiment for 256-bit ECC and a word size of 64-bit incorporating a prime number having 256 bits.

In this embodiment,

$N=B^4-B+n_0+B^4-n_0'$; $2^9 < n_0 < B$.

The operands have to be in normal space.

Then the reduction is done as follows:-

- Multiplication of n_0' by r_5 and adding r_1 (being step S20) with the new result called r_1;
- Multiplication of n_0' by r_6 and adding r_2 and the carry c of the previous multiplication (step S21) with the new result called r_2.
- Multiplication of n_0' by r_7 and adding r_3 and the carry c of the previous multiplication.

  Moreover r_4 is added to the upper part of the multiplication (step S22). The step consists of the lower half again called r_3 and the upper half q.
- Multiplication of q by n_0' and adding r_0 and adding the new r_1 to the upper part (step S23);
- When the last multiplication gives an overflow, the overflow is added to r_2 (step S24);
- When this again gives an overflow, it is added to r_3 (step S25);
- When this gives again an overflow, n_0' is added (step S26).

The carry of the third multiplication (q) is used as multiplicand and in the next multiplication, and can be enlarged by 1 bit.

Figure 5 is a block diagram of a hardware implementation of the present invention having the following components:

- X-,Y-,U- and Z-registers 10 to 13 for storing the input operands X, Y, U and R respectively;
- C- and R-register 14,15 for storing outputs C and R;
- RAM 16 for storing the intermediate results;
- Multiplier 17 which performs the operation B.C+R=X*Y+B*U+Z+c;
- State machine 18 which controls the operations and the transport between RAM and registers or between registers.

Multiplier 17 calculates the product of X and Y and adds, if required, the previous carry c, which is internally stored. The result is split into two equal parts, Z being added to the lower half and U to the upper half.

The output of C-reg 14 can also be directly used as y-input (for example for q in Figure 2).

In another form the present invention is implemented by software running on a microprocessor with appropriate ALU's to provide add, subtract and shift operations, and shift registers.

CLAIMS

1. A method of performing a reduction operation in a cryptographic calculation, the method comprising selecting a modulus having a first section with a plurality of "1" Most Significant Word states and a second section which comprises a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and operating (S1-S5; S10-S12; S20-S26) a reduction operation on the modulus/multiple.

2. A method according to Claim 1 comprising effecting a plurality of multiplication operations (S1).

3. A method according to Claim 2 comprising effecting a plurality of multiplication operations followed by effecting a reduction operation (S1, S2).

4. A method according to Claim 3 comprising repeating the combined multiplication operations and reduction operation (S1, S2).

5. A method according to any preceding claim comprising using a multiple of the modulus/multiple.

6. A method according to any preceding claim wherein, when the last multiplication gives an overflow (S4), the overflow is added to a part of the selected number.

7. A method according to Claim 6 wherein, when the overflow addition step (S4) produces an overflow, then n_0' (S5) is added to the overflow.

8. A method according to any preceding claim, wherein the carry c between two adjacent multiplications is effected as the addend in the next multiplication (S2).

9. A method according to any preceding claim comprising monitoring the number of leading "1"s to determine if the number is less than (k-2).

10. A method according to Claim 6 comprising initiating the next calculation when the number of leading "1"s is less than (k-2).

11. A method according to any preceding claim the method comprising operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.

12. A method according to any of Claims 1 to 10 the method comprises operating 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

13. A method according to any of Claims 1 to 10 the method comprising operating 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.

14. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 13 when said product is run on a computer.

15. A computer program directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of any one or more of Claims 1 to 13 when said program is run on a computer.

16. A carrier, which may comprise electronic signals, for a computer program of Claim 15.

17. Electronic distribution of a computer program product of Claim 14 or a computer program of Claim 15 or a carrier of Claim 16.

18. Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus comprising means to select a modulus or a multiple of a modulus having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and means (10-17) for operating a reduction operation on the modulus/multiple.

19. Apparatus according to Claim 18 comprising means (10-17) to effect a plurality of multiplication operations.

20. Apparatus according to Claim 19 comprising means (10-17) to effect a plurality of multiplication operations followed by a reduction operation.

21. Apparatus according to Claim 20 comprising means (10-17) to repeat the combined multiplication operations and reduction operation.

22. Apparatus according to any of Claims 18 to 21 comprising means (10-17) to use a multiple of the modulus/multiple.

23. Apparatus according to any of Claims 18 to 22 comprising means (10-17), when the last multiplication gives an overflow, to add the overflow to a part of the selected number.

24. Apparatus according to Claim 23 comprising means (10-17), when the overflow addition step produces an overflow, to add n_0' to the overflow.

25. Apparatus according to any of Claims 18 to 24 (10-17) comprising means to effect the carry c between two adjacent multiplications as the addend in the next multiplication.

26. Apparatus according to any of Claims 18 to 25 (10-17) comprising means to monitor the number of leading "1"s to determine if the number is less than (k-2).

27. Apparatus according to any of Claims 18 to 26 comprising means (10-17) to initiate the next calculation when the number of leading "1"s is less than (K-2).

28. Apparatus according to any of Claims 18 to 27 with means (10-17) for 192-bit EEC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

29. Apparatus according to any of Claims 18 to 27 with means (10-17) for 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

30. Apparatus according to any of Claims 18 to 27 with means (10-17) for 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.

31. A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.

32. Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.

33. A method of performing a reduction operation in a cryptographic calculation, the method substantially as hereinbefore described with reference to, and/or as illustrated in, any one or more of Figures 1 to 5 of the accompanying drawings.

ABSTRACT

IMPROVED REDUCTION CALCULATIONS

An Elliptic Curve Crypography reduction technique utilises a prime number having a first section of Most Significant Word "1" states, with $N = n_{m-1} + N_1B+n_0$.

[Figure 2]

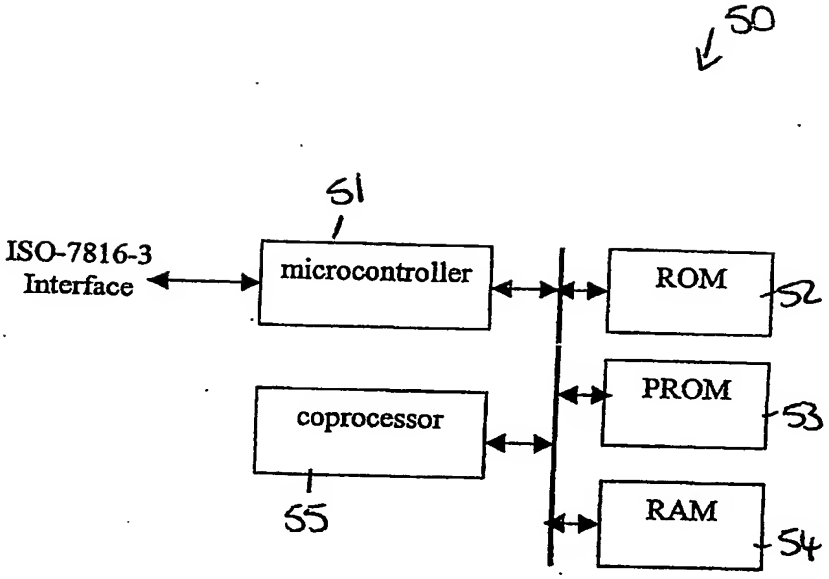
50
51
ISO-7816-3
Interface
microcontroller
ROM
52
PROM
53
coprocessor
55
RAM
54

Figure 1

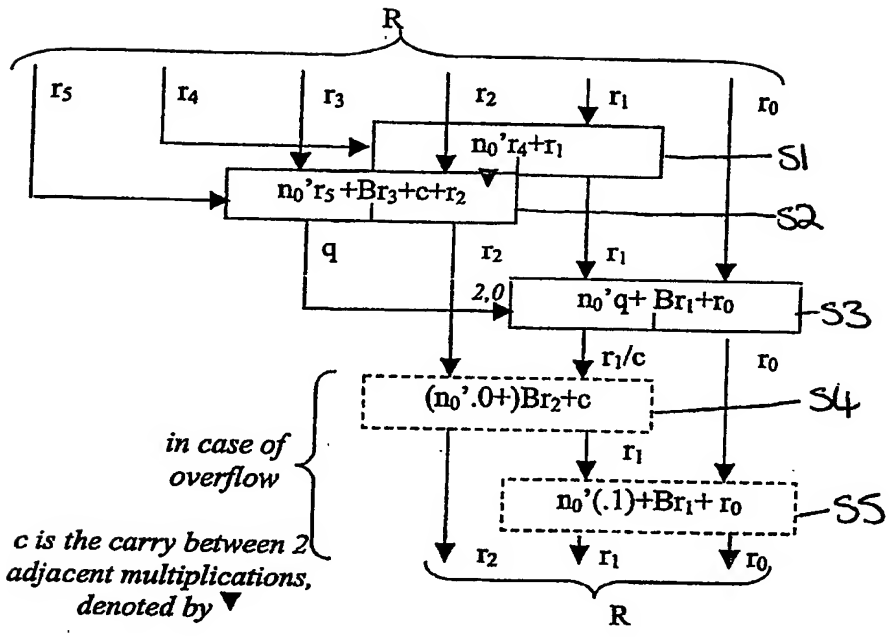
R
r5
r4
r3
r2
r1
r0
n0'r4+r1
S1
n0'r5 +Br3+c+r2
S2
q
r2
r1
2,0
n0'q+ Br1+r0
S3
r1/c
r0
(n0'.0+)Br2+c
S4
in case of overflow
r1
n0'(.1)+Br1+ r0
S5
c is the carry between 2 adjacent multiplications, denoted by
r2
r1
r0
R

Figure 2

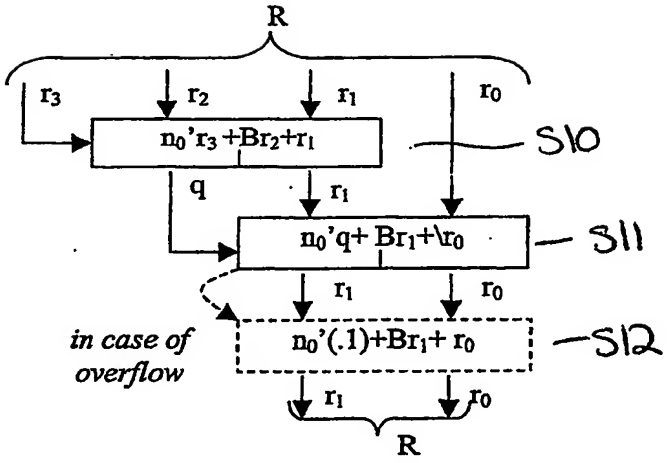
R
r3
r2
r1
r0
n0'r3 +Br2+r1
S10
q
r1
n0'q+ Br1+\r0
S11
r1
r0
in case of overflow
n0'(.1)+Br1+ r0
S12
r1
r0
R

Figure 3

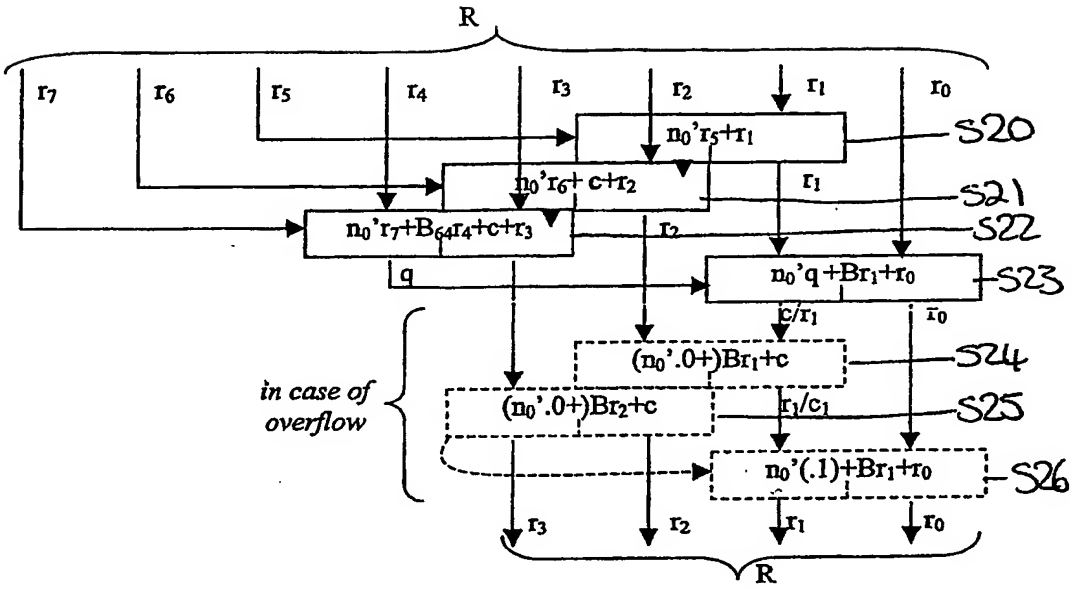
R
r7
r6
r5
r4
r3
r2
r1
r0
n0'r5+r1
S20
n0'r6+ c+r2
S21
n0'r7+B64r4+c+r3
S22
q
n0'q +Br1+r0
S23
c/r1
r0
in case of overflow
(n0'.0+)Br1+c
S24
(n0'.0+)Br2+c
r1/c1
S25
n0'(.1)+Br1+r0
S26
r3
r2
r1
r0
R

Figure 4

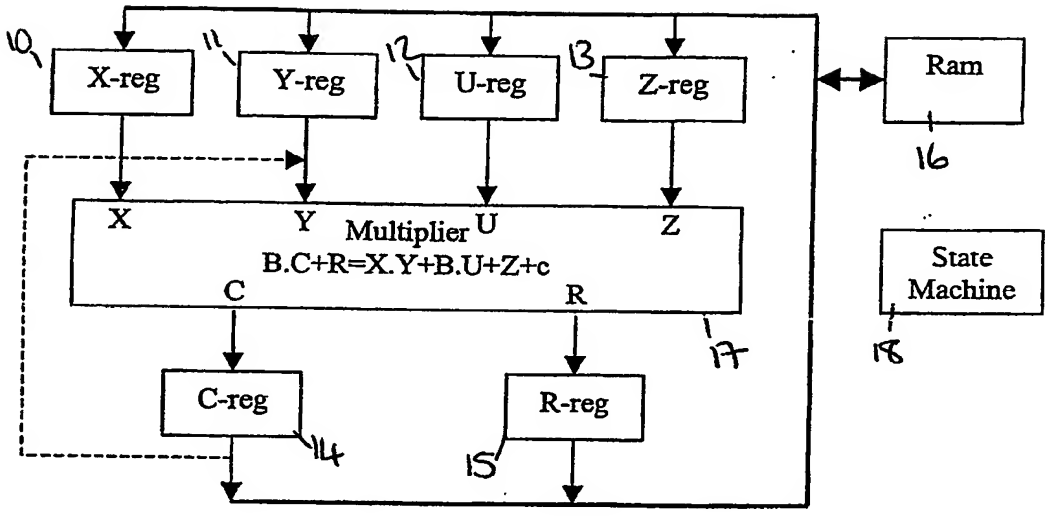
10
X-reg
11
Y-reg
12
U-reg
13
Z-reg
Ram
16
X
Y
Multiplier
U
Z
B.C+R=X.Y+B.U+Z+c
C
R
17
State Machine
18
C-reg
14
R-reg
15

Figure 5